

REMARKS

The present invention is a method of authenticating a user agent to a server using session initiation protocol messages and a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform a method of authenticating a user agent to a server using session initiation protocol messages. In accordance with embodiments of the invention, a method of authenticating a user agent to a server using session initiation protocol messages includes forwarding a SIP request from the UA to a server which may be a CSCF or a PCSCF; forwarding a request for authentication from the server to the UA in response to the SIP request which may be a SIP 401 unauthorized message or a SIP 407 proxy authentication request with the request for authentication including information that the authentication will be performed using a Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) mechanism; forwarding an authentication response from a user agent to the server in response to the request for authentication in accordance with the UMTS AKA mechanism which may be a SIP Register (authorization field) or a SIP Invite (proxy - authorization) and performing an invoked SIP procedure on the server in response to the SIP request if the authentication is deemed successful in view of the authentication response which may be a SIP 200 OK message of the call set up.

The specification stands objected to regarding the abstract and the informalities noted by the Examiner. The substitute specification submitted herewith addresses the informalities noted by the Examiner and amends the specification to improve its form for reexamination.

Claims 1-16 stand rejected under 35 U.S.C. §103 as being unpatentable over IETF RFC2543 (Handley) in view of 3G TS 33.102 further in view of United States Patent 6,477,644 (Turunen). These grounds of rejection are traversed for the following reasons.

The Examiner acknowledges that Handley does not explicitly disclose authentication associated with mobile systems including an UMTS AKA mechanism and an authentication response from the user agent to the server in response to the request for authentication in accordance with an UMTS AKA mechanism.

The Examiner's rationale that the aforementioned subject matter is obvious is that a person of ordinary skill in the art at the time the invention was made would find it obvious to combine the teachings of 3G TS 33.102 with the system of Handley because (1) mobile system UMTS builds on the success of the second generation mobile network GSM, (2) the UMTS AKA authentication parameters including the random number RAND, and authentication token AUTN are disclosed by 3G TS 33.102, (3) dynamically changing a new session authentication key similar to GSM has been used over ten years in the art as a strong security scheme to protect the sensitive information over the insecure open air space, (4) United States Patent 6,477,644 (Turunen) "discloses the security problem that the internet is not a secure network and it is possible for a third party to intercept internet traffic" and (5) Turunen "further discloses a way to improve security is to allocate new authentication to a mobile host whenever a mobile host makes new internet access request". It is submitted that this reasoning is based upon impermissible hindsight.

The fact that UMTS AKA is well known does not per se suggest, based upon the success of the second generation mobile network, the use of UMTS AKA in the context of the claimed invention which is limited to the use of the SIP protocol. As is stated on page 8 in lines 20-23 of the specification, the SIP standard defines three different techniques for authentication which are the HTTP basic authentication method, the HTTP digest authentication method and the PGP authentication mechanism. None of these known authentication techniques of SIP suggests to a person of ordinary skill in the art authentication as set forth in the claims with the SIP protocol using a UMTS AKA mechanism. Simply stated the fact that UMTS is the third generation of the GSM network does not suggest to a person of ordinary skill in the art to perform authentication in the SIP protocol using the UMTS AKA mechanism.

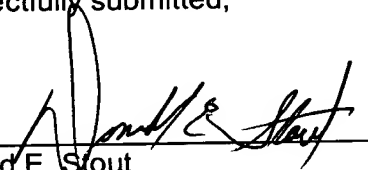
Moreover, the Examiner's reliance on Turunen does not cure deficiencies noted above with respect to the Examiner's basic reasoning that a person of ordinary skill in the art would combine Handley with the TS 33.102 version 3.5.0 to arrive at the claimed subject matter. Turunen does disclose that there is a problem with the Internet involving authentication/encryption keys which may be improved by allocating new authentication/encryption keys to a mobile host on a regular basis such as every time a mobile host makes a new access request. However Turunen's disclosure does not suggest anything pertaining to the authentication of UA with the SIP protocol and specifically how the SIP protocol may be authenticated using the UMTS AKA mechanism.

The dependent claims define more specific aspects of the present invention which are not rendered obvious by the proposed combination suggested by the Examiner.

In view of the foregoing amendments and remarks, it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 0172.38841X00) and please credit any excess fees to such deposit account.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Donald E. Stout", is written over a horizontal line.

Donald E. Stout
Registration No. 26,422
ANTONELLI, TERRY, STOUT & KRAUS, LLP

DES/kmh

Attachments

TECHNIQUES FOR PERFORMING UMTS (UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM) AUTHENTICATION USING SIP (SESSION INITIATION PROTOCOL) MESSAGES

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to techniques for performing authentication using SIP (Session Initiation Protocol) messages. More particularly, the present invention relates to techniques for performing UMTS (Universal Mobile Telecommunications System) authentication using SIP messages.

Description of the Related Art

The SIP has been selected as the protocol over the UNI (User to Network Interface), that is, the interface between the mobile subscriber and the CSCF (Call State Control Function), for R00 (release 2000) and the current UMTS AKA (Authentication and Key Agreement) is one proposal for the authentication mechanism for the R00 UMTS.

The SIP has been defined in the IETF (Internet Engineering Task Force) draft standard RFC2543 (Request For Comments), issued March 1999 and the UMTS AKA has been defined in the 3GPP (3d Generation Partnership Project) specification TS 33.102, version 3.5.0, Release 1999, issued July 2000. The contents of this draft standard in

its entirety and the contents of this specification in its entirety are both incorporated by reference herein.

As stated in the draft standard:

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. The sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these.

SIP invitations used to create sessions carry session descriptions which allow participants to agree on a set of compatible media types. SIP supports user mobility by proxying and redirecting requests to the user's current location. Users can register that current location. SIP is not tied to any particular conference control protocol. SIP is not designed to be independent of the lower-layer transport protocol and can be extended with additional capabilities.

However, the use of the UMTS AKA procedure to perform authentication through SIP messages has not been disclosed in the draft standard.

Furthermore, in the IP Multimedia (IM) subsystem, which supports mobile IP telephony, a subscriber authentication mechanism must be standardized. Such an authentication mechanism has not yet been standardized. However, the UMTS AKA procedure will most likely be the chosen authentication mechanism. Therefore, a technique to perform UMTS AKA using the SIP protocol must be defined.

SUMMARY OF THE INVENTION

An object of the present invention, therefore, is to provide techniques for performing authentication using the UMTS AKA procedure and carrying the corresponding UMTS parameters through SIP messages. The authentication may be performed either by creating a new UMTS AKA authentication mode with the appropriate fields contained within an SIP message or alternatively, the authentication may be performed by reusing and adapting an existing authentication mode (e.g.-the digest mode or the PGP mode) of an SIP message.

Another object of the present invention, in the case of an IM subsystem, is to use SIP messages, which have been selected to be used as the call control protocol between the UE (User Equipment) and the CSCF, to carry the authentication parameters.

Still another object of the present invention is to reuse the UMTS AKA mechanism as a possible solution for the authentication procedure in the IM subsystem.

A further object of the present invention is to define which SIP messages and header fields are to be used to carry the UMTS authentication parameters in order to use the UMTS AKA mechanism for subscriber authentication in the IM subsystem and how to include the UMTS authentication parameters in the SIP header fields.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and a better understanding of the present invention will become apparent from the following detailed description of ~~example~~ exemplary embodiments and the claims when read in connection with the accompanying drawings, all forming a part of the disclosure of this invention. While the foregoing and following written and illustrated disclosure focuses on disclosing ~~example~~ exemplary embodiments of the invention, it should be clearly understood that the same is by way of illustration and example only and the invention is not limited thereto.

The spirit and scope of the present invention are limited only by the terms of the appended claims.

The following represents brief descriptions of the drawings, wherein:

~~Figure~~ Fig. 1 illustrates an example of data flow between an SIP UA (User Agent) and a CSCF.

~~Figure~~ Fig. 2 illustrates an example of data flow between an SIP UA and a CSCF.

~~DETAILED DESCRIPTION~~ DETAILED DESCRIPTION OF THE INVENTION

Before beginning a detailed description of the subject invention, ~~mention~~ discussion of the following is in order.

When appropriate, like reference numerals and characters may be used to designate identical, corresponding, or similar components in differing drawing figures. Furthermore, in the detailed description to follow, example sizes/models/values/ranges may be given, although the present invention is not limited thereto. In addition, elements may not be shown within the drawing figures for simplicity of illustration and discussion and so as not to obscure the invention.

~~Figure~~ Fig. 1 illustrates an example of data flow between an SIP UA and a CSCF . However, a Proxy server may be substituted for the CSCF. According to the security policies, when a UMTS AKA needs to be performed, (~~e.g.~~ for example at a call setup or at registration), UA in the UE sends a REGISTER or INVITE request to the CSCF or Proxy. The CSCF or proxy can accept the registration with the 200 OK message or ask for an authorization with the 401 Unauthorized response.

According to the aforecited 3GPP specification, in order to execute a UMTS AKA procedure, ~~to~~ two parameters must be sent to the user to authenticate it, namely, the RAND and the AUTN, and then the user will respond.

Therefore, the 401 Unauthorized response includes the WWW-Authenticate response header field which contains the required authorization scheme and related parameters. In performing the UMTS AKA procedure in accordance with a present invention, the WWW-Authenticate header includes the RAND (RANDOM challenge) and AUTN (Authentication Token).

After a 401 response, the UA may send a new REGISTER or INVITE request, which should contain the appropriate authorization information in the Authorization header field. In the case of the UMTS AKA procedure in accordance with the present invention, the Authorization header contains the authentication response RES (RES) or the synchronization failure parameter AUTS (AUTS) or an error code (for example, an error message can be sent if the MAC (Message Authentication Code) (MAC) is considered to be invalid).

Referring now to ~~Figure~~ Fig. 2, which illustrates proxy authentication after an INVITE request is presented, upon the UA forwarding an INVITE request to the CSCF, the CSCF may ask for an authentication with a 407 Proxy Authentication Required response. The 407 ~~response~~ contains a Proxy-Authenticate response header field which contains the required authorization scheme and related parameters.

After receiving the 407 response, the UA sends an ACK (acknowledgment) (ACK) response and may repeat the INVITE

request, the repeated request containing the appropriate authentication information in the Proxy-Authorization header field.

In the case of the UMTS AKA procedure, the Proxy-Authenticate header contains the same information as the WWW-Authenticate header and the Proxy-Authorization header contains the same information as the Authorization header.

Since this procedure can be used only when the UA sends a request, for example, when it initiates a call, the procedure cannot substitute for the authentication at registration.

Note that the REGISTER request, 200 OK message, and 401 Unauthorized response, as well as other parameters and elements contained in the above-noted discussion, are all clearly defined in the aforecited RFC2543 draft standard.

The aforecited draft standard defines three different techniques for SIP authentication, namely, an HTTP "basic" authentication mechanism and an HTTP "digest" authentication mechanism, and a PGP (Pretty Good Privacy) authentication mechanism. The HTTP authentication mechanisms are defined in the IETF draft standard RFC2617, issued June, 1999. The contents of this draft standard in its entirety are incorporated by reference herein.

While the three different techniques for SIP authentication are usable, for simplicity, the UMTS AKA technique may be advantageously used instead and the UMTS

AKA elements may be substituted for the elements used for the three other SIP authentication techniques without needing a format revision in the SIP standard.

Accordingly, in accordance with the present invention, a 401 Unauthorized response includes a WWW-Authenticate response header field which contains the UMTS AKA authentication vectors, that is, the RAND (RANDOM challenge) and the AUTN (authentication token).

After a 401 Unauthorized response, the UE ~~a~~ sends a new REGISTER/INVITE request which should contain the appropriate authentication information in the Authorization header field: ~~the authentication response (RES), a synchronization failure parameter (AUTS), or an error code~~ can be sent if the MAC ~~(Message Authentication Code)~~ is considered to be invalid.

Note that for a call setup, as will be discussed below, a 407 Proxy Authentication Required response may alternatively be used to carry the UMTS AKA parameters.

The present invention defines two ways to carry the UMTS AKA parameters in the SIP messages:

As noted above, the SIP standard defines three different techniques for authentication, namely, the HTTP basic authentication method, the HTTP digest authentication method and the PGP authentication mechanism.

Therefore, a new authentication mode, a UMTS AKA mode, could be defined with the necessary fields. Alternatively,

the existing modes can be reused and adapted in order to perform the UMTS AKA procedure.

In order to be able to use the UMTS AKA procedure for authentication in IM subsystems, it is necessary to define how the UMTS AKA parameters are contained within the SIP messages. A new authentication method or mode may be introduced to include the UMTS AKA parameters in SIP messages. Noted below is a new authentication mode in accordance with the present invention. The new authentication mode contains headers which have been made as short as possible.

The WWW-Authenticate response header, in the case of a UMTS AKA procedure, must be able to carry both the RAND and AUTN. Accordingly, one example of a simple format which may be used is as follows:

```
WWW-Authenticate = "WWW-Authenticate" ":" "UMTS" RAND
AUTN
RAND = "RAND" "=" RAND -value
AUTN = "AUTN" "=" AUTN -value
```

A hexadecimal format may be used for both the RAND and AUTN values.

The Authorization header, in the case of a UMTS AKA procedure, must be able to carry the RES value or the AUTS value. Accordingly, one example of a simple format which may be used is as follows:

Authorization = "Authorization" ":" "UMTS" RES | AUTS
| AUTH-REJECT

RES = "RES" "=" RES-value

AUTS = "AUTS" "=" AUTS-value

AUTH-REJECT = "AUTH-REJECT" "=" error-code

A hexadecimal format may be used for both the RES and AUTS values.

The Proxy-Authenticate response header plays a role which is essentially the same as that of the WWW-Authenticate response header and therefore, one example of a similar format which may be used is as follows:

Proxy-Authenticate = "Proxy-Authenticate" ":" "UMTS"
RAND AUTN

RAND = "RAND" "=" RAND-value

AUTN = "AUTN" "=" AUTN-value

Similarly, the Proxy-Authorization response header plays a role which is essentially the same as that of the Authorization response header and therefore, one example of a similar format which may be used is as follows:

Proxy-Authorization = "Proxy-Authorization" ":" "UMTS"
RES | AUTS | AUTH-REJECT

RES = "RES" "=" RES-value

AUTS = "AUTS" "=" AUTS-value

AUTH-REJECT = "AUTH-REJECT" "=" error-code

Thus, in the case of an authentication mechanism in accordance with the present invention for use in an IM subsystem, UMTS AKA authentication may be used as a new authentication mode.

Since HTTP's basic and digest authentication mechanisms have been defined for use in the SIP draft standard, as noted below, the portions of the SIP message reserved for the digest mechanism may be alternatively used in accordance with a present invention to carry the UMTS AKA parameters:

For example, the "nonce" field formally used by the digest mechanism may be used to carry the UMTS AKA concatenated RAND and AUTN values in a hexadecimal format.

Since the contents of the nonce field is implementation dependent, the length of the field must be large enough to carry the RAND and AUTN values. If this is not the case, the "opaque" field, defined in the draft standard, may be used to carry a portion of the UMTS AKA parameters.

The "response" field defined in the draft standard will be used for the UMTS AKA RES element. In case of a synchronization error, the AUTS will be included in the "response" field. The first character of the "response" field can indicate that the response includes the RES, the AUTS, or an error code. The RES and the AUTS may be in a hexadecimal format.

In authenticating with the SIP message portion formally used for the digest mode, an "algorithm" field which formally specified which algorithm to use to compute the digest (MD5 may be used by default), may, in accordance with the present invention, be used to inform the receiver that this is a UMTS AKA procedure and in this way, the receiver will understand that the nonce field actually carries the RAND and AUTN.

As noted above, the PGP mechanism has been defined for authentication use in the SIP draft standard. As alternative, this mode may be used in accordance with the present invention to carry the UMTS AKA parameters. That is:

The "nonce" field may carry the RAND and AUTN values.

The "PGP = algorithm" may inform the receiver that it is a UMTS AKA procedure.

The result will be included in the "PGP-signature". Since this field may be more than 200 bits long, some of the first bits of this field may be used to specify the type of result, e.g.-RES, AUTS, or error code.

This concludes the description of the example embodiments. Although the present invention has been described with reference to a number of illustrative embodiments thereof, it should be understood that numerous other modifications and embodiments can be devised by those

skilled in the art that will fall within the spirit and scope of the principles of this invention. More particularly, reasonable variations and modifications are possible in the component parts and/or arrangements of the subject combination arrangement within the scope of the foregoing disclosure, the drawings, and the appended claims without departing from the spirit of the invention. In addition to variations and modifications in the component parts and/or arrangements, alternative uses will also be apparent to those skilled in the art.

What is claimed is:

ABSTRACT OF THE DISCLOSURE

A technique for authenticating a user to a server using SIP messages includes ~~fewarding~~ forwarding an SIP request from the user agent to the server. The server then forwards a request for authentication to the user agent in response to the invite request, the request for authentication including information that the authentication will be performed using a UMTS AKA mechanism. The user agent then forwards an authentication response to the server in accordance with the UMTS AKA mechanism and the server then performs the appropriate actions to perform an invoked SIP procedure in response to the SIP request. The SIP request may include any standardized SIP request including an SIP INVITE request or an SIP REGISTER request. ~~The request for authentication may include one of an SIP 401 Unauthorized code or an SIP 407 Proxy Authentication Required code. The request for authentication should include UMTS AKA RAND and AUTN vectors, which may be included in an SIP WWW-Authenticate or Proxy-Authenticate response header field. The authentication response should include one of either a UMTS AKA RES code or an AUTS code or an error code.~~